UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/675,165	09/30/2003	Ernie F. Brickell	42P16807	5908

8791 7590 10/17/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
TRUONG, THANHNGA B	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 10/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/675,165	BRICKELL, ERNIE F.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Thanhnga B. Truong
AU2135

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/5,8;6/30;7/2/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the communication filed on September 30, 2003. Claims 1-19 are pending. At this time, claims 1-19 are rejected.

Information Disclosure Statement

2. The information disclosure statements (IDS) filed on April 05, 2004, April 08, 2004, June 30, 2004, and July 02, 2004. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements are being considered by the examiner.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Proudler et al (US 2003/0226031 A1), and further in view of Ober et al (US 6,959,086).

a. *Referring to claim 1:*

i. Proudler teaches:

(1) receiving a request to prove that a platform possesses cryptographic information from a certifying manufacturer **(paragraphs 0065-0066 of Proudler);** and

(2) performing a direct proof by the platform to prove that the platform possesses the cryptographic information, the direct proof comprises a plurality of exponentiations each being conducted using an exponent having a bit length no more than one-half a bit length of a modulus (n) **(paragraphs 0065-0066 of Proudler).**

ii. Although Proudler teaches a trusted device as shown in Figure 8 and paragraph 0037, Proudler is silent on the capability of using an exponent

having a bit length no more than one-half a bit length of a modulus (n) in his cryptographic information proving. On the other hand, Ober teaches:

(1) Selection of symmetrical key length is the second step (Block 4). The key management method supports several key lengths depending on the symmetrical block algorithm. The key length can be adjusted between the preferred range of about 40 bits and about 192 bits, depending on the PCDB programming. For a standard DES and Triple DES, keys can preferably have about a 40 bit to a about 192 bit key length, programmable in 8-bit increments by the application. This allows for variable key lengths other than the typical 40, 56, 112, and 192 bit key lengths found on the market. The third step (Block 6) of symmetrical key generation can preferably be performed six ways: 1) sample the output of a random number generator to assemble the desired length DEK; 2) sample the output of the random number generator to assemble the desired length KEK; 3) perform Diffie-Hellman g.sup.xy exponential in order to arrive at a shared secret value, such as based on ANSI X9.42; 4) derive a symmetrical secret key by hashing an application supplied password or passphrase; 5) transform a key using a combination of hashing, mixing with fixed data and re-hashing, XORing, etc.; or 6) import a RED key provided by the application. The fourth step (Block 8) involves representing the secret key in one of preferably three ways: 1) inter-operable external form; 2) IRE (the encryption chip manufacturer) external form; or 3) IRE internal form. Numbers 2 and 3 are used to enforce the security policy, and Number 1 is used to allow shared key material with any other vendor's implementations. The symmetrical key inter-operable external representation step should be used when an application chooses to exchange the chip manufacturer's secret key with another crypto vendor. The secret key should be converted from the chip manufacturer's storage format into one that is more easily extractable so that it can inter-operate with other crypto vendors **(column 3, lines 22-57 of Ober).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Proudler with the teachings of Ober for creating a trusted environment **(paragraph 0001 of Proudler).**

iv. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Proudler with the teachings of Ober for Increasing the level of trust in platforms therefore enables greater user confidence that the platform and operating system environment behave in a known manner **(paragraph 0006 of Proudler).**

b. *Referring to claim 2:*

i. The combination of teaching between Proudler and Ober teaches the claimed subject matter. Ober further teaches:

(1) wherein the bit length of the exponent being at most 160 bits in length **[i.e., the key length can be adjusted between the preferred range of about 40 bits and about 192 bits, depending on the PCDB programming (column 3, lines 25-27 of Ober)].**

c. *Referring to claim 3:*

i. The combination of teaching between Proudler and Ober teaches the claimed subject matter. Ober further teaches:

(1) wherein the modulus (n) being over 1000 bits in length **[i.e., the modulus cannot be fixed, and a new modulus must be generated for each new public key pair (column 4, lines 25-26 of Ober). In addition, the modulus, public key and private keys can be exported/imported from/to the CryptIC. The public key is composed of two pieces: the public key (y) and the modulus data (p,q, and g). The CryptIC will allow a modulus size to be between 512 and 2048 bits with increments of 64 bits (column 17, lines 28-31 of Ober)].**

d *Referring to claim 4:*

i. The combination of teaching between Proudler and Ober teaches the claimed subject matter. Ober further teaches:

(1) wherein the bit length of the exponent being a constant value despite any increase in value of the modulus (n) **[i.e., the key length**

can be adjusted between the preferred range of about 40 bits and about 192 bits, depending on the PCDB programming (column 3, lines 25-27 of Ober)].

e *Referring to claim 5:*

i. The combination of teaching between Proudler and Ober teaches the claimed subject matter. Ober further teaches:

(1) wherein the bit length of the exponent being less than one-eighth the bit length of the modulus (n) **[i.e., the modulus cannot be fixed, and a new modulus must be generated for each new public key pair (column 4, lines 25-26 of Ober). In addition, the modulus, public key and private keys can be exported/imported from/to the CryptIC. The public key is composed of two pieces: the public key (y) and the modulus data (p,q, and g). The CryptIC will allow a modulus size to be between 512 and 2048 bits with increments of 64 bits (column 17, lines 28-31 of Ober)].**

f *Referring to claim 6:*

i. The combination of teaching between Proudler and Ober teaches the claimed subject matter. Ober further teaches:

(1) wherein the plurality of exponentiations conducted are of the form h.sup.t mod P, where "h" is a unique number, "t" is randomly chosen between an interval between 0 and W, "P" is a large prime number, and W is a number between 2.sup.80 and the square root of n **[i.e., the public exponent is created by finding an e that is relatively prime to .quadrature.(n), the product (p-1)(q-1). The starting point of this search is 65537. In most cases e remains 65537. In the event that .quadrature.(n)=65537k, where k>=1, then the encryption exponent will be the next largest odd value which is relatively prime to .quadrature.(n). The private exponent is found by taking the multiplicative inverse of e mod (p-1) (q-1) (column 18, lines 48-55 of Ober)]**.

f. *Referring to claims 7, 13:*

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

g. *Referring to claim 8:*

i. This claim has limitations that is similar to those of claim 5, thus it is rejected with the same rationale applied against claim 5 above.

h. *Referring to claims 9, 14, 18:*

i. These claims have limitations that is similar to those of claim 2, thus they are rejected with the same rationale applied against claim 2 above.

i. *Referring to claims 10, 15:*

i. These claims have limitations that is similar to those of claim 3, thus they are rejected with the same rationale applied against claim 3 above.

j. *Referring to claims 16, 19:*

i. These claims have limitations that is similar to those of claim 4, thus they are rejected with the same rationale applied against claim 4 above.

k. *Referring to claim 17:*

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

ii. Proudler further teaches:

(1) a bus; a network interface card coupled to the bus; and a processor coupled to the bus **[i.e., as illustrated in Figure 2, the motherboard 20 of the trusted computing platform 10 includes (among other standard components) a main processor 21 with internal memory 25, main memory 22, a trusted device 24, a data bus 26 and respective control lines 27 and lines 28, BIOS memory 29 containing the BIOS program 28 for the platform 10 and an Input/Output (IO) device 23, which controls interaction between the components of the motherboard, the keyboard 14, the mouse 16 and the VDU 18. The main memory 22 is typically random access memory (RAM) (paragraph 0045 of Proudler)].**

l. *Referring to claims 11, 12:*

i. These claims have limitations that is similar to those of claim 6, thus they are rejected with the same rationale applied against claim 6 above.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Lawman et al (US 2003/0028807) discloses a trusted device, physically associated with a network appliance that does not include a CPU, communicates with at least one component of the appliance and is accessible via a network connection to the device for providing a signal indicative of a condition of the appliance (see abstract).

b. Wiseman et al (US 2004/0003288 A1) discloses an apparatus may include a root of trust for measurement (RTM) module coupled to a verified platform security property policy module and a comparison module (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Thanhnga B. Truong
AU2135

TBT
October 10, 2006